Army S&T Investment In Interoperability

By Charles L. Barry

Center for Technology and National Security Policy

National Defense University

January 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Army S&T Investment In Interoperability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**32**	

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

Charles L. Barry is a Senior Research Fellow at CTNSP and President of Barry Consulting, Inc. He is a retired Army officer with extensive experience in joint and multinational operations. His areas of expertise include international relations, U.S. military strategy, joint command and control, land warfare, and information networks related to command and control. Barry received his doctorate in Public Administration with a concentration in Information Resource Management from the University of Baltimore. He also holds a BA in political science from Loyola University, Chicago.

Acknowledgements. The author wishes to acknowledge Dr. Thomas Killion, Army S&T Executive, and Dr. Hans Binnendijk, Director of the Center for Technology and National Security Policy at the National Defense University for their support of this project. Dr. Richard Chait, Dr. John Lyons, and Mr. Albert Sciarretta are also acknowledged for their comments and suggestions during the research on and development of this report. Appreciation is also extended to Samuel Greene, CTNSP intern 2008, for his review of the final draft of this paper.

Contents

Executive Summary

Requirements that Army systems be interoperable add cost to any program from its very inception, from applied research and development to program milestones and ultimate manufacture and fielding. Program funding estimates from the beginning of concept design and engineering must highlight the added costs associated with meeting various interoperability requirements.

Designing interoperability requirements into systems is complex. It begins with an understanding how the technology application sought and the system design being selected will operate with all other systems on the battlefield. Interoperability must be evaluated in the context of Army and Joint Service doctrine that sets forth how systems are to be employed in a joint, multinational or interagency operation. However, the most basic interoperable requirement is internal – backward compatibility is interoperability with other Army systems.

Understanding interoperability requires technical knowledge of agreed standards and architectures as well as knowledge of the relevant systems of other Services, key allies (such as Canada, the UK and Australia), and the Army's most likely interagency partners. The context thus understood provides an accurate picture of how future Army systems (or upgrades to existing ones) must be designed for effective interoperable performance. This applies to software programs as much or more so that hardware programs.

The most critical interoperability systems are those that link forces together, that provide secure and continuous network integration, both voice and data. These are the networks that support the six operational functions of: command and control: intelligence, fires, movement and maneuver, protection and sustainment.

Most if not all costs associated with adding interoperability to system designs can be identified through program analysis resource management methods already in use by Army PA&E. The S&T specific costs thus isolated form the basis of an evaluation of return on developmental cost invested in interoperability features.

The primary quantitative metric for assessing the interoperability value-added are the number of interoperable systems produced as a percent of overall Army systems interoperability requirements. This metric can be further defined in terms of interoperable capabilities for joint, multinational and interagency as well as Army-internal interoperability.

A key cost-benefit question is, "How much interoperability is enough?" This is especially relevant in the multinational arena where allies from many different nations may have numerous systems, each of which would require costly compatibility features to be added to a new Army system. How often and how many Army elements require interoperability with infrequent allies? In some cases the more practical solution will be to temporarily rely on tried and proven liaison teams for connectivity. The S&T decision maker must consider the concept of decreasing marginal returns when reflecting on the potential

numbers of systems required and the investment in, for example, networking all echelons beyond their immediate local area needs: Does every platoon or squad leader require worldwide connectivity?

The cost of maintaining interoperable potential is especially salient for software systems. These systems often require regular patches and upgrades to perform as intended. When multiplied across many interface protocols, the maintenance cost can be substantial in terms of running technical support.

Interoperability with a civilian agency poses relatively new concerns. Most civilian agencies use commercial systems that may be difficult to connect to Army technologies for procedural and policy reasons as well as technology. However such connectivity has become more critical in theaters such as Iraq and Afghanistan. The Army needs more research on technological solutions to this requirement. However, the only immediate solution may be continued investment in commercial off the shelf systems for Army users who have to interoperate with civil agencies.

This paper discusses the elements of assessing ‘bang for bucks’ with regard to S&T investment in interoperability. It intends to point to where interoperability investment offers the greatest return and to open our thinking to the possibility that universal interoperability of all systems is not a desirable or attainable goal, especially when allocating investments and accepting reasonable risk.

Chapter 1. The Context for S&T Interoperability Investment

The future of national and international security lies in interoperability and cooperation among the Services, the interagency, international partners and non-governmental organizations. Each Service brings to the fight unique and critical capabilities, but those capabilities are only as good as the contribution they make to the overall strategic effort. Nobody goes it alone today.

CJCS Guidance for 2007-2008, 1 October 2007.
Admiral Michael G. Mullen, U.S. Navy, incoming Chairman of the Joint Chiefs of Staff

What operational value does the Army realize from its S&T investment in interoperable systems, in particular, the investment in network systems that support the functions of battle command and intelligence sharing? Where does S&T investment in interoperability provide the greatest return on investment? How much interoperability is enough?

The Army invests substantial S&T dollars to make its forces interoperable, most critically through reliable communications and information sharing: voice and data networks; technology and data standards; as well as common applications and formats for command and control along with other combat functions.

Systems interoperability begins inside the Army though the requirement for backward compatibility of new technologies with legacy systems. However, interoperability must also extend to compatibility between the Army and the systems of the other Services, allied military forces and—more recently—with civilian agencies of the U.S. government and other civilian entities, especially in post conflict operations.

This paper attempts to answer the opening questions above, or at least provide a useful framework for their consideration. First, it explores the importance of interoperable capabilities in terms of Army doctrine and concepts - how the Army fights today and plans to fight in the future. It will examine core doctrine and emerging concepts to establish the principle that interoperability is an essential design feature of any S&T investment and network systems in particular. It will point to high payoff interoperability investment areas, most notably operational network connectivity. It will base its analysis on the four broad categories of S&T interoperability design: intra-Army systems compatibility, inter-Service joint interoperability, interoperability in a multinational coalition setting, and interoperability with civil agencies and partners in stabilization and reconstruction operations.

The main premise underlying this analysis is that interoperability among coalition forces is essential, and therefore a value to be prioritized and measured in making S&T investment decisions. A model is put forth, using a priority program in the area of C4 networks, to quantify interoperability improvement achieved though S&T investments that enhance the interoperable features of networks, either intra-Army or joint or multinational. The analysis proceeds with a scheme for assessing and visualizing when S&T investment in interoperability reaches a point of decreasing marginal returns; when

further investment approaches the region of diminishing utility relative to life cycle cost. Along the way we will discuss how to isolate cost factors related to interoperability, and how to aggregate them.

The study concludes with observations and recommendations for further research, including S&T investments not related to networks that will enhance interoperability. S&T managers and decision makers, aware of the essentiality of interoperability as well as the high opportunity costs of designing systems that are not interoperable, can better examine investment proposals in basic as well as applied research, and in systems design engineering. They need to know, "If our research and development investment is successful, will the new system play well with others on the Army's core team?"

Interoperability and Army S&T program design

Why focus on interoperability in seeking to improve the Army's return on its S&T investments? Because system interoperability is an imperative consideration of every S&T program design, beginning with the initial concept phase. Long tested and refined doctrine on how the Army employs its forces establishes that systems be interoperable with other U.S. forces and adhere to NATO and other international agreements such as the Multinational Interoperability Council on standards. Doctrine is derived from experience and experimentation, and is promulgated to leaders and soldiers at all levels as how best to conduct their tasks. It describes the plays in the Army playbook; mission planning then selects and draws together plays into a coherent operational plan on how a force is to achieve a given objective. Scientific research and technology development that aims to equip the Army has to develop systems that support how the Army fights; these activities also must discover new technologies to help evolve doctrine over time. The doctrine of interoperability applies across all organizational levels.

Today's operational Army sees itself as a fully integrated team, in spite of the constant fielding of new systems or upgrades of older ones that creates a continuous struggle to mate old and new capabilities together as one team. At a higher level of organization the Army is a member of the U.S. military's joint force, which seeks full integration but realistically is comprised of four Services working together with varying degrees of advanced interoperable capabilities. The U.S. joint team, in turn, almost always operates as the core of a larger multinational military team; a team that usually enjoys no more than rudimentary interoperability, such as unclassified or lower classified levels of voice and data communications over limited legacy networks. This multinational military team is often further partnered with essential civilian agencies and organizations in an internationally sanctioned operational environment, such as PRTs in Afghanistan. Civilian organization may come from among the U.S. interagency cohort or from international agencies or even non-governmental communities. These agencies are important partners when, inevitably, mission success requires a host of undertakings beyond just combat operations. Unity of effort among the Army's own elements, with joint and multinational military forces, and by interagency/international partners furthers mission effectiveness, resource efficiency, and risk reduction. Wherever and whenever necessary the Army and its teammates must be able to work together smoothly, based on integrated training, prior planning and deployment of the best connective systems.

However, interoperability requirements are cost factors in S&T design as well as value features of the systems produced. Interoperability means adding specifications to program design, which in turn triggers added research and manufacturing investment, whether the program is basic research, FCS, C4I, RSTA, indirect fires, direct fire systems, soldier systems, or logistics. Production costs are direct and identifiable. S&T interoperability costs, whether invested in physical design modifications or software developed to DOD and internationally agreed standards, may be more difficult to define and assign, even though much of those costs are traceable as well. Design and testing costs can be isolated accurately through well-established program analysis and evaluation tools. Examples of interoperability-related systems design costs include added weight to UAV systems, or the interoperability-related investments required by additional code for programmable multi-channel radios or interfacing different Blue Force Tracking systems. Some costs are not so readily assigned. However, they can be allocated methodically, and if done with sufficient consistency will provide useful comparisons for investment decisions.

Information networks are the highest value interoperability systems for Information Age operations. Information interoperability specifications are technologically complex and fast evolving. The additional cost of designing systems to achieve information interoperability can be categorized into four distinct investment arenas:

- Interoperability to achieve backward compatibility and connectivity with existing or legacy Army information systems.
- Adding features to comply with Joint force interoperability consistent with U.S. military doctrine, in particular, network interface standards as defined by relevant documents,[1] including data architecture standards. The usual reference to Joint force interoperability means interface with appropriate elements of the Air Force, Navy and Marine Corps plus Coast Guard.
- Incorporating multinational interface standards for compatibility with standing alliance and coalition networks as defined by international agreements. These specifications are agreed with other members of several groups to which the U.S. military belongs, including the North Atlantic Treaty Organization (NATO), the Multinational Interoperability Council (MIC), ABCA and others.[2]
- Including features to network with civilian agencies, international organizations and local governments. The standards employed in these arenas are often based on market-dominant commercial technologies over which restricted networks can be operated. Networking with these groups is a new but growing requirement and the sources of specifications vary widely by agency. S&T designs will not often include capabilities to link to these networks due to internal (i.e., Army or DOD)

[1] Relevant documents include the latest version of the Joint Technical Architecture, which encompasses the MIL-STD 188 Military Communications Systems Technical Standards series, and DOD Instruction 4630.8, Procedures for Interoperability and Supportability of Information Technology and National Security Systems" (2004).

[2] NATO standardization agreements (STANAGS) date to the earliest days of the Alliance in the 1950s and continue to be promulgated, advising all current 26 members. In contrast, the MIC and ABCA standards organizations (see footnotes 32 and 33 respectively) have far fewer members and act as informal, more agile groups for advancing broader interoperability standards related to command and control.

classification restrictions, however, the requirement still remains important in some cases.

However, as already stated, interoperability not only raises system cost, it is also a value eagerly sought. Interoperability of Army systems with air and maritime transport platforms – design compatibility, ease of on load/off load, securing of vehicles, etc – reduces deployment times. Interoperability between sensors and shooters increases combat effectiveness by timely target engagement. Interoperability of information systems (focused at present on data exchange modeling) improves situational awareness, collaborative planning and success in execution. Apart from any other quantifiable value-added, a system's capability to interoperate with other task-related systems can be identified as an increased return on investment. For example, an Army indirect fire controller that is designed to link with other Service or allied UAVs adds considerable value for indirect target engagement. The question is: how can investment decision makers quantify the interoperability return of dollars invested?

The S&T decisionmaker has to determine, among other factors, the 'interoperability quotient' of a new technology or system—when and how a particular investment makes the system a measurably better team player, or conversely, reduces team play by introducing less interoperable (or even non-interoperable) systems into the inventory. First, the decision maker must have a good understanding of how the system might be employed based on current or evolving doctrine. It is often said that joint operating capability resides more in Service cultures and procedures than in the equipment that science and technology investment can provide. Interoperability is also about psychological buy-in to the concept of a 'larger integrated team' – thinking beyond Army programs alone. That buy-in is still being learned by many. In deciding how to equip the future force, both culture and science must come together.

Summary

It has been over 20 years since passage of Goldwater-Nichols; and all Service cultures have internalized the value of joint operations and written those values into their doctrine and concepts. Today, even the most senior Army leaders know no other doctrine than joint military operations. Yet declared goals for inter-Service jointness have yet to be achieved. Some Army and Marine Corps Blue Force Tracking systems do not interoperate; many voice and data systems remain proprietary; airspace coordination over the battle space continues to be debated. Progress now depends on overcoming the last tough issues so the team can truly work together as one: Service investing in interoperability as a priority, and further compromise on matters such as airspace management and on network control and integration procedures. It requires more effective S&T investment to provide systems that overcome obstacles to cooperation, whether the obstacles are process-based Service equities such as network control or real obstacles such as effective integration of all desired airspace users in a tactical battlespace. Making the investment decisions to reach the optimum measure of interoperability will require Services to assign a higher value to broad systems integration throughout the R&D process.

The Army and its fellow Services need procurement processes that ensure no incompatible system—whether MILSPEC, COTS, MOTS or any other profile—can degrade interoperability or become an obstacle to future joint operations. Conversely, when technology *is* able to ensure interoperable capabilities, there are times when the requisite decisions to invest in those capabilities are not taken because adding interoperability features drives up unit cost. Waivers to requirements are sought to speed acquisition or to avoid a reduction in the number of systems affordable under a fixed or shrinking budget. Still other systems find their way into the inventory under rapid fielding initiatives or field commander's initiative funding, in spite of contractors proprietary designs or features (including training and supportability) that cannot be replicated in the wider force.

One readily quantifiable measure of the return on investment (ROI) in new systems is how well they comply with Joint and NATO architectural standards. If they are fully compliant, the ROI from an interoperable perspective should be considered high, perhaps even 100%. Partial compliance or noncompliance with joint or multinational standards would rate accordingly.

A key element in enhancing joint interoperability or even interdependence among Services is the ease (including upgradability attributes) with which new technologies integrate into existing Service, Joint, Multinational and Interagency networks. This is being facilitated by migrating toward data sharing methodologies and interface protocols rather than discreet proprietary software or hardware systems. The move to data standards versus systems standards is a positive development as it de-couples standards from proprietary systems: so long as the data is readable the software or platform can be from any source. That is especially useful for systems that are fielded in subsequent updated models, each operating different versions of software. Yet data tagging and dictionaries require continuous updating and are not a stand alone solution.

At some point the Army must consider whether networking every soldier to the global network enterprise, or designing every Army platform to interface with any possible allied legacy network architecture, are worthy investments. Local networking might provide joint integration "good enough" for lower echelons. For rare coalition partners with antiquated systems, old fashion liaison teams might be the best investment, allowing S&T investment to be directed to where greater ROI yields for the same dollars can be realized. In short, the Army needs to specify jointness and interoperability goals to be achieved, rather than proceeding on the simple assumption that networking every system to every other system is the end game for joint or multinational interoperability. Service-wide blanket connectivity is likely a goal never to be realized and may not be wise. Fielding timelines alone dictate that Army leaders will always have to manage some level of system dissimilarity. Indeed, full interoperability at every level and for all unit types might not be the greatest ROI for the Army.

Chapter 2. The Army's Commitment to Interoperability

It is worth reviewing the Army's cultural evolution, from its initial heritage as a stand alone force to its place today as a fully integrated joint team member. By doing so those supporting our front line forces in the S&T community can better grasp the permanence and invasiveness of the Army's multi-level interoperability requirements.

The Army's interest in joint operations is almost as old as the Army itself. Occasions of inter-service cooperation have occurred since the earliest days of the Republic, though they were neither often nor close in terms of synchronization. The Continental Army fought alongside the French Army and with the support of the French Navy during the American Revolutionary War, most notably at the final siege of Yorktown. During the Civil War both the northern and southern armies employed naval support for bombardment, troop transport, and supplies. Naval support of Union engagements occurred throughout the war around the Chesapeake Bay, along the southern Atlantic coast and throughout inland waterways, notably at the siege of Fort Donnellson, the Battle at Shiloh, and the campaigns against Vicksburg and Chattanooga.[3]

The Spanish-American War of 1898 was one of the most significant turning points in Army-Navy relations. Until that war, the Army had maneuvered to and sustained its own forces in almost every battle fought since 1776.[4] However, getting to the battlefields of the Spanish-American War required naval deployments to Cuba, Puerto Rico and the distant Philippines. The war with Spain heralded a permanent strategic shift from continental to overseas employment of U.S. land forces. Ever since, the Army has needed the Navy—and later the Air Force—not only for initial deployment and eventual redeployment, but for continuous sustainment of all of its land campaigns.

Painful difficulties in coordination between the Departments of War and the Navy during the Spanish-American War and ensuing insurgency in the Philippines prompted creation of a Joint Army and Navy Board in 1903 to improve future collaboration. However the Board proved powerless and had no affect on subsequent operations in World War I. A larger Joint Army-Navy Board was instituted in 1919 that managed to produce the first joint operational publication in 1935. But like its predecessor, that effort too lacked directive authority and had no influence on World War II operations.

World War II saw organization of a de facto U.S. joint staff in an attempt to smooth out inter-Service rivalry and effect joint planning. By the end of the war America's military leaders were convinced future operations must be conducted jointly. General Dwight D. Eisenhower, the Army Chief of Staff in 1945 noted that a high price had been paid in blood that could be traced to Service parochialism and that "separate ground, air, and sea warfare is gone forever."[5] A permanent Joint Chiefs of Staff was included as a prominent feature of the National Security Act of 1947.

Many modifications of that historic legislation were made in subsequent years, each striving toward further development of joint capabilities but meeting limited success

[3] See Personal Memoirs of U.S. Grant for accounts of Army-Navy cooperation in Vol I, Chap XXX-XXXIX and Vol II, Chaps XLIV, LVI, LXI and LXV.
[4] A notable exception was the seaborne campaign against Vera Cruz and onward to Mexico City in 1847-48.
[5] "A Word from the Chairman," Joint Forces Quarterly #12, Summer 1996, 1

because Services still set exclusive criteria for promotion to the highest ranks and had all but unfettered allocation of their own funding for investment. The failure of the needlessly complex and overly compartmented four-Service Operation Eagle Claw (1980) in Iran, followed by technical and procedural obstacles in inter-Service communications during Operation Urgent Fury (1983) in Grenada, led to Congressional investigations and eventual legislation. The most well known law later enacted is the Goldwater-Nichols Act of 1986. That Act, among other provisions, strengthened the role of the Chairman of the Joint Chiefs of Staff relative to the Service Chiefs, and required every future general or admiral to have served in a joint assignment prior to selection for that rank.[6]

Army Jointness in the 21st Century

Since Goldwater-Nichols the Army and its sister Services have made impressive if initially hesitant strides toward genuine joint operating capabilities. The rise in prominence of the Joint Staff and the Chairman has been equally beneficial to the emergence of joint operations. Twenty years after Goldwater-Nichols there is a wealth of joint doctrine ("Joint Pubs") under which Service doctrine is aligned. Today, forces in Iraq and Afghanistan perform as true joint teams and are fully integrated in many ways. One can often hear in the Pentagon halls today, "the Army gets it" on joint operations. Joint operational capabilities have become more of a reality and not mere jargon. One recent example of inter-Service teamwork is the highly regarded bi-service Army-Marine Corps doctrinal manual on counterinsurgency published in 2006.[7]

However, much work remains for the Army and other Services to be joint in all important ways. Even the core function of communicating continues to witness disconnected users. The teaming of Army units with other military forces and non-military agencies requires, at even the most rudimentary levels of cooperation, the capacity to exchange information. At more sophisticated levels of interoperability or even integration with other forces, systems must be technically compatible and reciprocally supportable. The newest stated goal is to strive for interdependency with other forces, such that the Army, at least tactically, can depend entirely on selected capabilities of other Services for some essential elements of combat power, foregoing any self-support capability. An example would be deploying land forces without fire support assets or UAVs, which would be made available from other Services. Rapid universal voice and data exchange remains an elusive goal.

Through its training and education programs the Army has raised a generation of leaders fully immersed in the joint doctrine noted above, flowing from an array of Joint Publications. Yet calls for closer integration and interdependent operations have intensified. The reliable, secure and instantaneous exchange of high volumes of time-critical data is one concern. Streamlining logistics and deployment times is another. Working with allied forces in closely coordinated battles and with civilian agencies in delicate peace operations are other new requirements—if not on their face, certainly in their details. Battle Command, operational tempo (Otempo), simplicity, and teamwork for

[6] The formal title of the G-N Act is the 1986 Department of Defense Reorganization Act.

[7] The manual, titled "Counterinsurgency" and dated 15 December 2006, is known as both Army Field Manual 3-24 and Marine Corps Warfighting Publication 3-33.5

multi-Service or multinational operations are expected to mirror the close teamwork of Army-only operations.

That goal remains far-off. The Army still has limited capacity for genuine integrated operations with the other Services, and only a low level of interoperability with some of our allies. Network interoperability with civilian partners—a more recent concern—is only in its infancy. Making progress *toward* interoperability is not the only challenge in assessing the ROI of S&T program investment proposals. The Army must also guard against moving *backward* toward less "jointness" when it invests in new systems and technologies that can de-couple the Army from existing networks.

The Army's growing interest in interoperability dictates that all future systems will have to prove they are interoperable to the extent required by doctrine and agreed standards. S&T decision makers, like others engaged in determining the highest return from limited resources, must understand not only the requirements for network interoperability but the value added that can be obtain from any given program. What are the requirements, generally speaking, that can be used to assess programs? For a deeper look, we will return to our four tier model of interoperable forces and marry those groups to the doctrine just discussed.

Chapter 3. Connectivity in Joint, Interagency and Multinational Operations

Information Age operations place a premium on the interoperability of information networks, systems and technologies. Assured instantaneous exchanges of secure information in voice, data, or visual form across networks regardless of Service, nationality, or uniform will be the essential core of interoperability in 21st Century warfare. With networks as the life blood of interoperability, the highest priority S&T investments should relate to the functions of Battle Command. These are technologies that provide advantages in communications and computing systems from the strategic to the tactical level to help commanders visualize, decide, and direct operations. The second priority should be systems related to intelligence, surveillance, and reconnaissance (ISR); without the intelligence function commanders and staffs would be working from a much-degraded operational picture. Finally, Army S&T priorities directed at interoperability should invest in systems that provide logistics interoperability, including standardized transport, sustainment, and medical systems. The Army must be able to access logistics from other Services as well as allies and commercial sources. Standardized RFID technology, bulk items such as fuel and ammunition, plus sensitive medical services and supplies fall into this category.

Interoperability Standards and S&T Investment

Standards warrant further scrutiny in terms of their impact on interoperability costs. In short: standards are the beating heart of interoperable technologies.[8] They are essential to interoperability and have a long history of attempted management both within DOD and with key allies. Yet establishing agreed standards takes time and compromise. It also requires strong top-down emphasis in order to maintain consistency and control cost.

Military leaders can take one of three paths in selecting standards. They can identify a problem and call for solution options from which to select. They can opt for commercial solutions. Finally, they can direct that a unique standard be developed to meet the military need. The first and third of these are similar; however the difference lies in pre-determining that a non-conventional solution is necessary.[9] According to the Joint Technical Architecture, DOD supports an open system architecture where all systems comply with a single interface standard.[10] The JTA also mandates that "all standards must be stable, technically mature and publicly available." As a result, most DOD standards are commercial or industry standards.[11] If standards are too narrow and detailed, such as

[8] However standards are readily eclipsed by extant factors such as institutional culture, doctrine and training in achieving genuine interoperable organizations. It is well recognized that technical interface alone does not make allied forces interoperable. For scholarly treatment of this point, see *Mind the Gap*, Gompert, David C. et al, NDU Press: Washington, 1999. pg. 37.

[9] See *Standards—the Rough Road to the Common Byte*, Libicki, Martin C. NDU Press: Washington, May 1995. Pg 23.

[10] Ref. JTA Volume 1, Version 6 (2003). Accessed 10 August at http://handle.dtic.mil/100.2/ADA443891

[11] Joint Technical Architecture (JTA): Standards for Interoperability, briefing by Judy Kerner, Aerospace Corporation at the Software Technology Conference, 1 May 2002. Slide 16.

exclusive military specifications (MILSPEC), many powerful and worthy technologies from the commercial-off-the-shelf (COTS) world will be prohibited. As a result, the JTA requires all new systems to include a 'Technical View' comprised of all relevant standards in the latest version of the JTA. Older technologies are deleted via a 'sunset' process intended to avoid the cost of incorporating all the oldest interface protocols in every new system. The JTA's Technical View is subject to compliance at every milestone decision of the Defense Acquisition process.[12]

All this sounds like DOD and the Army have standards under control; however there are traps the S&T community should guard against. One is continued preference by many vendors for proprietary software, such that once acquired, the Army is often stuck with follow on systems from that vendor (or perhaps a limited number of others) due to incompatibility problems. This is a persistent problem. Vendors are reluctant to expose their technologies to competitors. Therefore strict compliance with the JTA is critical to achieving wider interoperability. Lower S&T costs with a non-compliant vendor could actually reduce future interoperability or drive up down stream costs to maintain it.

As with most regulations, the JTA includes procedures for waivers from standards if compliance poses undue burdens in terms of cost, development timelines or acquisition processes. Given these broad reasons, the waiver option is used more often than hoped. Another source of waivers is operational requirements. Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) have increased demand for the rapid acquisition of leading edge technologies and their fielding to units in or deploying to combat areas. Technologies may even be purchased from vendors by local commanders in order to provide the best systems to soldiers heading into battle. Under these circumstances the compliance systems moves into a 'catch-up' mode: the pace of technology development moves much faster than the institutional process of updating the JTA. One part of the solution is for the S&T community to stay current with the JTA's relevance to applied R&D programs, and to identify when new technology goes beyond its reach. A goal should be to compress standards updates to better serve the warfighter with the latest interoperable technologies without creating down stream gaps.

Terms of Reference Related to Interoperability.

Interoperability presents a number of different variables which can be compared and contrasted when seeking to assess returns on technological investments. The basic question is how much does it cost – discreetly – to interoperate at all the following levels, and how much is that worth to the Army? What are the tradeoffs when investment resources are (almost always) limited? In short, what does the Army gain from its S&T investment in interoperable capabilities?

- Intra-Army Combined Arms Team. This is the most basic building block of interoperability: "the full integration and application of two or more combat arms or elements of one Military Department (Army) in an operation (JP 3-18).
- Joint (usually referred as 'jointness'). Joint operations are operations of two or more Military Departments (i.e., Services) operating under a single Joint Commander, or Service operations supported or working together with another

[12] See DODI 5000.2 "Operation of the Defense Acquisition System" dated 12 May 2003.

Service (see JP 1-02 for Joint Force and Joint Operation). Recent interest at TRADOC indicates that Joint interoperability is extending to also mean interoperability between general purpose forces (GPF) and Special Operations Forces.

- Interoperability. The traditional building block of jointness is interoperability. JP 1-02 the DOD Dictionary, defines interoperability as "the ability to operate in synergy in the execution of assigned tasks the capacity to work together in the field. Interoperability is not a term intended to apply exclusively to multinational operations, though it is often used in that context; it applies to all force compositions.
- Integrated Operations. An unofficial description intended to deepen interoperability especial for information operations to a level where decisions about equipping the operational force is determined predominantly by joint Combatant Commands, with procurement, training and sustaining still implemented by the Services.[13]
- Interdependency. This emerging concept not yet fully or officially agreed. In one sense it is used to describe a concept of joint force employment that goes beyond interoperability or integrated operations to achieve a conceptual combination of dominant maneuver and precision engagement across all levels of warfighting—tactical, operational, and strategic. The theory is to present a dual threat to an enemy, e.g., destruction by fires and maneuver simultaneously.[14]—In a more current application it is being discussed as a concept where Services are able to forego certain internal capabilities by agreeing that another Service's provision of that capability is so responsive and complete that the Service being supported becomes fully, or at least more fully, dependent on the sister Service's capability. In turn, the supported Service is able to forego some of its internal capability investment and thus reduce redundancy in areas such as air delivered munitions.
- Interagency coordination—"… the coordination that occurs between elements of DOD and engaged U.S. Government agencies for the purpose of achieving an objective." (JP 3.0 page GL-18).

Network Enabled Operations

The concept of Network-Centric Warfare (NCW) was spawned around 1996 by Admiral William Owens, then the Vice Chairman of the Joint Chiefs of Staff. It grew to prominence in 2001 under the late Vice Admiral (Ret) Arthur Cebrowski, who headed the OSD Office of Force Transformation. Over time the concept underwent several evolutions. First, it expanded to encompass operations other than warfare, becoming Network-Centric Operations and Warfare (NCOW).[15] Later, perhaps to simply the

[13] For an analysis of joint force integration see "Extending the User's Reach" by David Gompert, Charles Barry and Alf Andreassen, Defense & Technology Paper 24, CTNSP, National Defense University, February 2006. Also see Richard Downie, *Defining Integrated Operations*, Joint Forces Quarterly #38 Summer 2006, 10-13.

[14] See Antulio Echevarria *Interdependent Maneuver for the 21st Century* Joint Forces Quarterly #20, Summer 2003. pp 21-26*e*

[15] See DOD *Network Centric Operations and Warfare Reference Manual (NCOW RM)* Version 1.1, 17 November 2005.

process of selling the complex concept to allies, the name was changed to Network-Centric Operations (NCO), where it officially remains today in DOD literature, including the 2006 Quadrennial Defense Review (QDR). The principal tenet of these related concepts is that once fully networked, the network created will impart greater combat capability than the systems populating the network. Put another way, future joint force capability will become network-centered rather than platform-centered.

However, allies have challenged the NCW/NCO theory's principal tenet. Some European allies instead pushed a variant called"Network Enabled Operational Capabilities." In NATO forums, where the United States and Europe meet on military issues such as common doctrine and operating concepts, the name became Network Enabled Operations. Australians also preferred that name.[16] And the U.S. Army appears to be one of the skeptics.[17] In a 2005 essay the current Commander, TRADOC, then LTG William Wallace declared that networks were enablers for commanders and staffs to gain situational understanding from subordinates, intelligence sources and other systems. Situational understanding enabled the commander to visualize an operation, decide on and communicate an operational intent, and to direct actions that will achieve that intent and operational success. Neither the term NCW or NCO are contained in the September 2006 Joint Publication 3.0 Joint Operations. Nor are these terms contained in the Army's December 2006 FM 3-24 (Counterinsurgency Operations) or the new Army FM 3.0 (Full Spectrum Operations), published in February 2008.

From the evolution above it is possible to conclude that the Army's real metrics for interoperable networks can be measured in terms of their capacity to enable core combat functions, especially command and control and intelligence, but also fires, movement and maneuver, protection, and sustainment.[18] Therefore, ROI metrics for network systems research, as with other system initiatives in S&T, can be tied to enhancements of these core functions.

Army Interoperability with the other Services: "Jointness"

Beyond the concept of networks, the Army has internalized the concept of Joint operations in its doctrine, concepts, planning, and education systems. That is the good news. The 'rest of the story' is that the inherent pace of modernization across scores of systems means that even internally the Army will always face a situation of less than full technical interoperability. When the M-1 Abrams tanks were first fielded they had to operate in tank-infantry teams with the much slower and more vulnerable M-113 APC, which also used different fuel. When the UH-60 Blackhawk helicopter was fielded it was initially protected by the much slower, less powerful, and more vulnerable AH-1S model Cobra gunship. After the initial fielding of the Blue Force Tracker system began to generate operational feedback, newer versions incorporated more advanced information that commanders began to rely on during planning and execution, only to find that when

[16] See Dr. Carlo Kopp, *Understanding Network Centric Warfare,* in Australian Aviation, January/February 2005. Accessed on 22 February 2008 at http://www.ausairpower.net/TE-NCW-JanFeb-05.html

[17] See Lieutenant General William S. Wallace, USA, *"Network Enabled Battle Command"* in Military Review. May-June 2005. pp 2-5.

[18] These six functions are identified as the core joint operational functions common to all operations at all levels of war. See JP 3.0 Operations. Pg III-1.

operations mixed newer and older versions of BFT they had to be satisfied with the less capable information the older systems were limited to. These and similar situations among the Services are common and require staffs and commanders to continuously address and work around disconnects in interoperability. Staying as interoperable as possible requires constant attention across the operational force. It also requires attention in the area of new technology development.

The Army in Multinational or "Combined' Operations

The Army conducts operations with allies for political as well as military reasons. In Operation Urgent Fury, the invasion of the minor island (133 square miles) of Grenada, a 5000 strong U.S. joint force was augmented by about 300 troops from the security forces of several neighboring island states. The only operation in recent times that was solely a U.S. unilateral operation was the 1989 invasion of Panama (Operation Just Cause).

America's most capable and sizable allies for multinational operations have been its the North Atlantic Treaty Organization (NATO) partners, Australia and South Korea. In addition to its long operating history with NATO during the 45 year Cold War, NATO allies later fought alongside the U.S. Army in Bosnia, Kosovo, Afghanistan, and Iraq. No group of nations provides a richer or more dependable source of potential operational partners. Similar comments apply on a smaller but still potent scale to Australian, South Korean and New Zealand forces.

In the most critical area of Communications and Information Systems (CIS) interoperability, NATO considers four levels:

- Level 4: Seamless sharing of information - integrated data transfer applications
- Level 3: Seamless sharing of data—common data exchange model
- Level 2: Structured data exchange—manual and automated read
- Level 1: Unstructured data exchange—manual read only

At present, NATO assesses that most all allies are at Level 2 and NATO realistically holds Level 3 as its midterm goal. NATO has set numerous new standards in the area of CIS, including use of the Internet since the end of the Cold War. However new standards are only applied as member states invest at the national level in those standards in their next generation CIS equipment. Often national budgets delay or prevent complying with new standards; hence actual progress toward capabilities is far slower than agreeing to standards at the NATO policy level.[19]

NATO has also agreed to a host of other measures toward collective operational interoperability over the course of its nearly 60 years of existence, including collective management and funding of its own Alliance networks under the NATO Consultation, Command and Control Organizations (NC3O) and its components. Much still remains to be achieved at the national level, especially among newer members struggling with many competing economic demands for investment. Nonetheless, NATO is the most prominent

[19] For an in-depth analysis of NATO CIS interoperability see Charles Barry *"Transforming NATO Command and Control for Future Missions"* Defense Horizons Paper 28, CTNSP, National Defense University, June 2003.

source of allied cooperation in multinational operations, as can be seem from the lists of allies contributing to Operation Iraqi Freedom and NATO's taking command of the International Security Assistance Force in Afghanistan since 2003.

The Army and Civilian Teams_The foremost operational scenarios where the Army anticipates working with interagency partners is stability operations, including post-conflict, peace enforcement, humanitarian assistance and disaster recovery environments. DOD Directive 3000.05 [20] is the primary guide for investment in capabilities to work with and support interagency teams. It calls on the Army to develop its own stability operations capabilities, as well as to ensure that research and development (R&D) and acquisition programs support stability operations. In addition, it directs that the Army "supports interagency requests for personnel and assistance to bolster the capabilities of U.S. Departments and Agencies to conduct stability operations…"

The Directive also states that stability operations are a core mission of the U.S. military and are to be "given priority comparable to combat operations..." The implementation of the Directive will take some time to put in place. Meanwhile, the Army and the other Services are taking a number of ad hoc initiatives to work with other federal agencies, including through exercises. In theater cooperation is also taking place in Iraq and Afghanistan. Ideas for S&T investments related to interagency interoperability will come out of these experiences. What is already clear is that this is an enduring requirement.

[20] DOD Directive 3000.05 "Military Support for Stability, Security, Transition and Reconstruction (SSTR) Operations" dated 28 November 2005

Chapter 4. Measuring Interoperability Return on Investment for Army S&T

Can we measure system interoperability in a way that allows assigning a cost to such features? The premise here is, 'Yes.' This chapter proposes one method, based on four postulates about equipping the Army to be interoperable:

Postulate 1: Joint interoperability is a value that can be quantified by the number of critical platforms (systems) and headquarters (nodes) that are interoperable throughout the Army, with other Services, allied militaries, and civilian partners.

Postulate 2: Existing analytical methods can and do break out costs of individual component features of new systems, including S&T costs related to required interoperability features of systems, including software. Such cost-related features provide new or upgraded systems with the ability to interoperate.

Postulate 3: Doctrine—how the Army plans to fight - drives the definition of interoperability requirements with other Services, allied militaries, and civilian partners in various systems, and thereby provides a reliable assessment tool for determining where interoperable systems are of greatest value in the execution of operations.

Postulate 4: The value of interoperable systems can be established quantitatively by measuring interoperability goals in terms of the numbers of desired systems able to work together to the design standard.

Basis Example of ROI quantification

- Example: A Primary Ground Vehicle Voice Communications System
- S&T Investment Cost: *q*
- Number of systems in inventory projected through 2020[21]: *x*
- Desired percent of systems to be interoperable with other Services:[22] 90% *x*
- Desired percent of systems to be interoperable with allied force systems:[23] 50% *x*
- Current number of systems interoperable with other Services: 70% *x*
- Current number of systems interoperable with allies: 30% *x*
- Desired or anticipated number of interoperable systems/upgraded systems to be realized by S&T investment in new systems: *y* (20% increase).
- Number of systems/percent increase in inter-Service interoperability realized by S&T investment in new systems: $x + y = z$ (90% = inter-Service interoperability investment goal).
- Desired or anticipated number of interoperable systems/upgraded systems to be realized by S&T investment in new systems: *r* (20% increase).
- Number of systems/percent increase in interoperability realized by S&T investment in new systems: $x + r = s$ (50% = allied interoperability investment goal).

[21] Since investments are usually projected over a FYDP (the Pentagon is presently working on the FY09-14 FYDP), the inventory time parameter must be six years or longer. 10-15 years is more realist given common program stretch outs.

Second, as shown in the template above, we identified interoperability goals for the entire inventory of systems in a particular category, including systems already being procured. Finally, the added interoperability provided to Army forces by the new system is assessed. The vehicular communications system example above illustrates the cost association model, depicting interoperability requirements for both joint and coalition interoperability.

Several factors need elaboration at this point in the hypothetical example. First, while S&T investment is but one cost center in systems development and acquisition, it can typically be identified as a discreet system-related investment, either for systems under development or as costs to be assigned in future (perhaps on a shared basis) to systems yet to be designed. In the latter case the identification of costs as interoperability related may have to await future systems development and fielding. Should no system materialize these costs may be a lost investment. Second, the generic example given above poses a new vehicle voice radio system that will add interoperability simply by the numbers acquired. Another scenario could be created by retrofitting technologies to older systems without increasing the overall numbers. Yet another investment strategy may add value by enhancing the quality of interoperable communications. Each situation calls for establishing different quantitative metrics in measuring ROI. For example, increasing the numbers of voice radio systems that include interoperable secure voice communications can be quantified against a target number of systems or units with that capability.

Another factor for costing consideration is the impact of interoperability investment on the overall inventory of voice radios (in this example). As a new system is designed, care has to be taken not to "de-couple" the interoperability of older legacy systems and so devalue interoperability.

In some cases these factors are just the tip of the analysis. The decision maker must also be aware of other investment decisions pending, both inside the Army modernization program and the programs of other Services and allies. It would be a foolish investment indeed that achieved connectivity with systems that are to be replaced in the near term, or to deploy technology that is being overtaken by even greater capabilities. This last point may seem obvious but experience suggests that it is not. For example, the Joint Tactical Radio System (JTRS) now coming into the inventory incorporates technology designed up through 1996 when the original JTRS design was approved. Difficulties in program development have caused long and unexpected delays; while newer software designed radios with many JTRS capabilities have begun to show up in the military market place.

Cost Case Study: Investing in Blue Force Tracking (BFT) Interoperability after Fielding

The Army's Blue Force Tracking (BFT) technology grew out of the Enhanced Position Location Reporting System (EPLRS) first fielded in 1999. BFT uses Global Positioning System (GPS) technology and communications links to display the positions of BFT-

[22] Joint capable would mean interoperable for its primary functions, e.g., secure voice and data with all other Service systems that Joint Doctrine indicates it should be compatible.
[23] Based on NATO systems architectural standards.

equipped friendly units on computer displays of other BFT equipped vehicles and command centers.[24]

The first BFT, deployed in 2002, was an EPLRS-based line-of-sight limited technology, integrated into the Army's Force Battle Command Brigade and Below (FBCB2) command and control system. It was intended to enhance situational awareness for commanders from division down to battalion. At the same time the Marine Corps received BFT technology designed to different specifications in order to incorporate it into the Marine command and control system known as Personal Computer Command and Control (PC3). The systems were immediately popular with commanders but not compatible across the two Services.

The compatibility issue grew. The Army, needing beyond-line-of-sight BFT capabilities developed a SATCOM-based version for use over extended distances, began to field a SATCOM linked version of FBCB2/BFT to forces in OIF/OEF in 2003. Later the Army system would be deployed to Air Force JSTARS aircraft to allow air support command and control to see supported land forces. Over time, as many as nine different BFT technologies and systems have been fielded for different needs, including Special Operations Forces (SOF) and the Services.

These systems use varying combinations of operating systems, interface protocols, and application software. Even within the Army many different systems remain incompatible today. In August 2003 the Joint Requirements Oversight Council (JROC) directed the Army to take the lead in development of a single joint system. This system is forecast to also be shared with a limited number of allies, notably forces of the United Kingdom.

The new system, called the Joint Battle Command-Platform (JBC-P) has finally been approved and is to begin fielding in late 2008. The Army is to eventually field 120,000 JBC-P systems while the Marine Corps plans to field 20,000. The updating or replacement of current Army and other Service BFT systems will take place over the next five years and is estimated to cost $1.7 billion.[25] Meanwhile, the popularity in the field of BFT grows, with design of handheld and dismountable versions as well as plans to mount a version of the system similar to versions already on helicopters on UAVs. Displays, messaging, and latency refresh cycles will be improved.

The S&T reflection on this case study is to ask, "Could the years and considerable cost being invested today in making the BFT system interoperable have been reduced had the Army invested in and required vendors to adhere to BFT interoperability standards during initial development?" Over the next several years (if funds are not cut) the BFT case will become a 'hindsight' look at engineering inoperability into a system after field use demonstrates the demand. Yet the requirement for situational awareness, the tenets of joint warfighting doctrine, and incidents of friendly fire all pointed to the requirement long before the first BFT systems were developed. The BFT case shows clearly the high cost of *not* incorporating interoperability in the initial funding of S&T programs.

---

[24] See McCarter, Mickey, "Army expands use of technology that identifies friendly forces on and above the battlefield" in Military Information Technology Online Archives, Volume 8, Issue 4. Jun 17, 2004. accessed 23 Feb 08 at http://www.military-information-technology.com/print_article.cfm?DocID=504

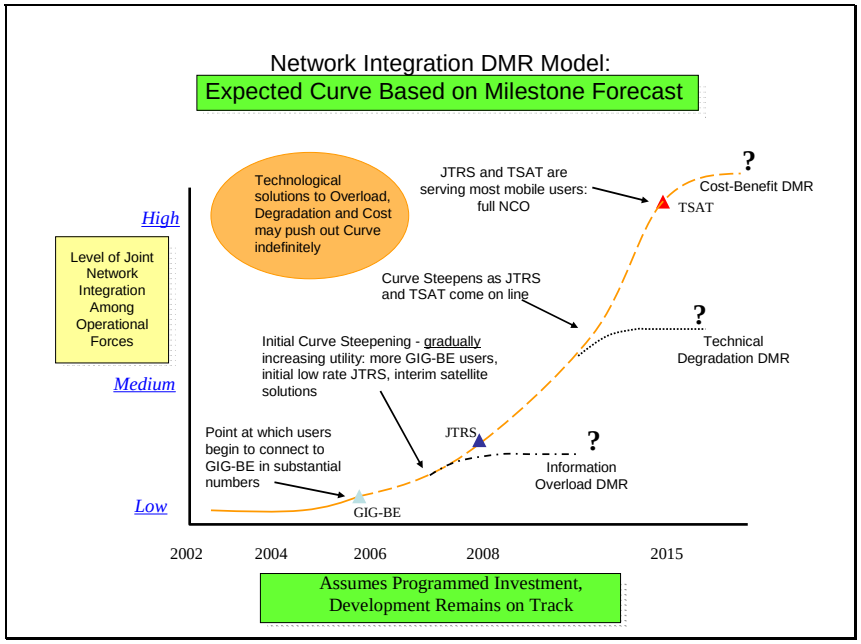
[25] Osborn, Kris, "U.S. Army, Marines to Share Tracking Data", *Defense News*, February 4, 2008. pg 6

Chapter 5. Decreasing Marginal Returns: How Much Interoperability is Enough?

How much joint capability does the Army need? To what level should forces be networked horizontally to other Services in addition to traditional hierarchical command structures? In October 2001 newswires carried the photo of a U.S. Special Operations soldier riding horseback across the plains of northern Afghanistan and communicating with a B-52 bomber 30,000 feet overhead, about to deliver tons of precision-guided bombs on Taliban forces.[26] A tremendous display of joint capability; but how many soldiers does the Army want to invest in networking to B-52's?

The Network Centric Warfare (NCW) goal has been to ensure 'all information on the network should be available to anyone who requires it, instantly and at any time.'[27] Yet the well-established Law of Decreasing Marginal Returns might be examined in considering the cost of Army-wide networking of every soldier to all other service members and allies.

Consider the example illustrated in Figure 1 below, which depicts acquisition of the Joint Tactical Radio System (JTRS) that coupled with the Tactical Satellite (TSAT) system should connect all soldiers to the Global Information Grid (GIG). As more soldiers are connected, the unintended consequences of information overload, technological



degradation of the network due to increased user population, and higher cost of sustaining such a communicating system must be weighed against the value (returns) of having all

[26] As told by Secretary of Defense Donald Rumsfeld in remarks before National Defense University students, 31 January 2002. *http://www.defenselink.mil/speeches*

[27] Discussion with Mr. Terry Pudas, former acting Director, OSD Office of Force Transformation.

soldiers connected. Often soldiers only need to connect to local tactical networks, not the global information grid, either directly or indirectly. At a minimum, decisions to invest in doing so should be carefully scrutinized and determined on a wholesale level.

Army Investment Priorities to Enhance Joint Capabilities

In similar fashion, the Army should consider the level of integration that is needed to work with the other Services, other militaries, and with the interagency. Decisions now need not be cast in stone but should be revisited as operational experience accumulates. The following is a good point of departure is establishing S&T investment priorities for interoperability.

C4. The most critical focus for joint, multinational and interagency operations—you have to be able to communicate in real time or near real time.

ISR. The second most critical element for jointness is the capability to share real time intelligence.

Fires. Units need fires for mission prosecution and force protection, fires from air systems, and indirect land systems of any Service or ally. When fires are needed, they are usually needed right away.

Logistics. Other Services of the U.S. military by and large have adequate logistics of their own. However, the Army has Title 10 responsibilities to the other Services for discreet support. For example, the Army provides theater postal service, mortuary affairs, ground-based air defense, and other services to all forces in a particular area of operations. Today, approximately 25,000 Army personnel provide support to the other military Services in the OIF theater of operations.

Assessing JIIM Interoperability Improvements Generated by Army S&T Investments

The first goal of decision makers in acquiring new systems should be borrowed from the oath of medical professionals, *primo no nocere* (first do no harm). In other words, new systems should not disconnect the Army from its essential joint partners. If the Army S&T investment is consistent with all agreed joint and NATO standards, and stays that way throughout development, its return on investment can be measured in the number of Army units with the latent capability for full joint and multinational operations. One way to quantify that is as a percent of units so capable before and after investment and fielding.

This is easier said than done. In the JROC review process for new systems two criteria are to determine if proposed systems are joint-ready and NATO standards compliant. Conceptually, adding features to systems in order to allow them to be compatible with other Service or NATO systems adds costs. These requirements may also add size and weight. In a finite program budget that may also face cost increases from other factors, adding cost to each unit translates into fewer units procured. Since “equipping the force” is the legislated duty of the Services, buying fewer systems is not a desirable goal. Therefore Service program managers have often sought waivers of requirements deemed nonessential, including requirements that new systems meet joint and NATO standards as

well as Service specifications. The Army should consider joint and NATO standards as congruent with Army standards.

Another difficulty arises from rapid fielding requests from Combatant Commanders or Service leaders and commanders at every level. Commanders may become aware of a new prototype system with valuable enhanced capabilities over what is on hand. No one wants soldiers to deploy with second best technology when a better known product is available, even if it lacks compliance with Joint architectures and specifications. Waivers are often requested at a high level, leaving staffs no option but to grant them and attempt to update to acceptable standards after the fact—until the next request comes along.

The most critical need for working together with partners from any of the JIIM populations is that the Army and its partners be linked by automated two-way information exchange. Assured, secure information exchange capabilities are most essential at the operational and tactical levels of war where time factors are most critical to mission success as well as force protection. Of course, there is no clear demarcation between these levels. However, being able to exchange information only at the top operational level or the lowest tactical levels alone would not constitute JIIM operational capabilities. The most common medium for automated information exchange are voice and data, with video rapidly gaining in equal status.

Chapter 6. Analyzing Army Doctrine to get S&T Investment Right

Army scientist and researchers, like other professionals, tend to stay in their lane; there is more than enough challenge in finding solutions within their disciplines. However, truly wise S&T investment depends on understanding the execution of interoperable joint, civil-military, and international operations. S&T decision makers have to perceive when S&T investment can push the execution envelope and provide an operational advantage in mission performance. What inter-Service, interagency, or international policies and agreements drive common operations? Who are the Army's primary or most likely operational teammates among the JIIM communities? Who supports whom? What are the requirements that underpin effective JIIM operations?

Keys Points on Joint Doctrinal Concepts

Army S&T decision makers and resource allocators must have solid understanding of joint doctrine as well as evolving Service roles and missions in order to select technologies or design systems that further joint interoperability. The Army's closest joint partner in land combat is the Marine Corps, for close air support it is the Air Force (but followed closely by Naval and Marine Air), and for strategic deployment and sustainment it is the Navy. Technological investments that strengthen these foundations of joint operations should be the Army's highest priorities.

Yet operations where Marine infantry operate inside Army BCT's, or the reciprocal, are rare. Technologies will have greater application if they can enhance the capability of land forces to instantly share information between units operating in close proximity—a situation that is far more critical for mutually supporting offensive or defensive operations, as well as force protection (preventing fratricide). In conventional operations the Army and Marines would not operate in such close proximity. The Marines and Army, while similar in many respects, have distinctly different roles and missions in U.S. national security, each valuable and essential but unique and usually distant. Not so in counterinsurgency warfare and stability operations, the grist of what is now called the 'persistent conflict' forecasted for U.S. forces over the next 10-20 years. Fresh Joint doctrine as well as agreed Army and Marine Corps doctrine explains how Marines and Army forces will fight together during this coming period.[28] Knowledge of what has been agreed with regard to how the force will be employed has to be part of the S&T decisional mix to achieve maximum interoperability value from limit investment.

Technologies that will help the Army interoperate with its battlefield air partners are more complex because air-ground operational combat systems have burgeoned in recent years. UAV's are the most recent category of airspace users over the battlespace; however, the emphasis on limiting collateral damage and force protection has intensified the precision required by all airspace users. Land force commanders at the tactical

[28] Perhaps the three most essential doctrinal publications for the Army S&T community to consider today are JP 3.0 "Joint Operations" (September 2006), Army FM 3-24/Marine Corps MCWP 3-33.5 "Counterinsurgency" (December 2006), and Army FM 3-7, "Stability Operations." These describe, respectively, how the Joint community intends to operate as a cohesive fighting force, and how the Army and Marine Corps agree to fight counterinsurgency operations.

level—where airspace use is the most intense both in terms of timing and space allocation—are justifiably unaware of the complexities of orchestrating multiple users onto the same target area without endangering friendly forces or civilians. Since the earliest days of aviation on the battlefield interoperability in this area has defied technological solutions. Today the same procedural separation of users is employed as existed in Vietnam and before, yet the demand for closer and closer parameters has grown exponentially. Army scientists working on technologies for automating integrated airspace use must understand not only inter-Service agreements on airspace control and procedures but also what solutions are being researched by other Services and even international research teams.[29]

The Army's interoperability with the Navy, while multifaceted like the other Services, is the most straightforward, except for airspace use by naval aviation and gunfire, which falls under the airspace user challenge already discussed.[30] In broad terms, the Navy deploys and sustains the Army when it operates overseas, as it has continuously for more than 100 years. Army personnel man port operations with the Navy and can be involved in integrated security operations. These are important but less challenging areas of interoperability for Army S&T investment. The Army must work with the Navy on rapid and efficient transport operations. This includes on load/off load systems for Army equipment; protection from maritime environments for sensitive Army systems such as helicopters, and optimization of deck space versus integrated Army unit loading (for rapid employment in the objective area). As the Navy looks to faster (e.g., smaller surface effects hovering and hydrofoil transports), more survivable, and more fuel efficient ships in the future, Army equipment designers need to be aware of and perhaps at times influence Navy designs.

Interagency, International and Multinational Interoperability

Understanding the roles and procedures of the interagency, international, and multinational arenas is far more difficult. The interagency realm has enjoyed intensified emphasis since the Iraq invasion. Yet thus far, Army interface with this community in terms of interoperability remains undefined beyond broad concepts. When and under what conditions does the Army cease being the supported force and become the supporting force? In the immediate aftermath of combat (which is rarely a discrete point in time or geography) the situation is often too uncertain for civilian teams to be useful. Instead, re-establishing public security, essential services and governance are skills the Army itself needs. Once civilians come forward to begin to assist Army commanders, they will be wholly dependent on Army resources in order to be effective.

[29] In the international arena the EU is investing in research to determine how to integrate UAV's into civil airspace. This is important for Army researchers for two reasons. First, what strategic agreements are reached first will often reduce options for follow-on systems that must integrate with existing systems and protocols. Second, Army UAV's operating in counterinsurgency environments often must integrate into civil airspace environments in support of civil-military operations, for example in restive but still functioning cities carrying on normal air operations. For more on the EU investment just getting underway see http://www.eda.europa.eu/newsitem.aspx?id=312

[30] The topic of Navy SOF operating with Army and other service SOF is a critical focus of Joint interoperability that is beyond the scope of this paper.

A key planning point is determining the level of support deployed interagency personnel require from the Army (or Marine Corps, coalition militaries), beginning with pre-deployment exercises and all the way to sustained operational cooperation in the field. What kind of kit does the Army expect interagency teams to acquire in order to operate with Army forces? What support does the interagency expect from the Army? How can S&T help solve these requirements: security, communications, transportation, and sustainment? Civilian interagency representatives may need unique communications gear that will generate logistical support requirements as well as bandwidth, computing support, and spectrum management issues. Additional transportation requirements for these teams may impact some future equipment designs, for example, vehicles with multiple communication interface mounts or vehicles that can expand to accommodate additional personnel. Can S&T lead to readily deployable shelters, low cost night vision systems, personnel tracking technology, and other equipment for support of sizable civilian interagency teams over sustained operations?

The international community includes international organizations (IOs), nongovernmental organizations (NGOs), and often local government institutions or officials. Interoperability with these communities is always unique and often situationally or personality determined. Still, operating with these partners, while problematic and sometimes contentious, is an essential feature of both counterinsurgency and stability operations, as well as disaster relief and other peace operations. The greatest interoperability return for Army S&T investment in this category will be lightweight low power streaming two way translation equipment and/or disposable cell phone and computer (for internet access and email) equipment. The Army should not be the primary source of this equipment for the international community. However there are times when operational success hangs on the capability to communicate. In those situations, the ROI can be measured on how many essential partners can communicate with Army commanders.

Finally, the Army's interoperability with allied militaries is an important factor in determining the value of S&T investments. At times the Army will need to consider tradeoffs in terms of its own technological advances and the ability to operate closely with other militaries. One historical example illustrates this point. When the Army upgraded its helicopter fuel ports in the 1970s to accommodate new rapid refueling technology existing manual refueling port were modified, restricting the space of the original manual fuel port to a smaller area in order to incorporate the rapid refueling adapter. The old design met agreed NATO standards for manual refueling equipment as NATO had no rapid refueling systems. The new design posed no problem so long as the helicopters refueled at Army sites because the Army acquired smaller manual nozzles for the restricted opening. However, NATO and even U.S. Air Force fuel trucks did not have such non-standard nozzles. When special nozzles were not available, as was the case for most NATO allies, fuel pressure had to be reduced to a trickle to avoid dangerous spills as the now-oversized NATO nozzles were used to refuel Army helicopters. The result: rapid refueling technology for the Army meant nearly doubling the refuel time required when using non-Army refuel points, and a loss of operational flexibility.

One of the key policy issues is the transfer of more advanced technologies and systems from the United States to even its closest allies. It is well established that the United

States has far outspent its potential allies in the area of S&T as well as procurement for many years. The technology investment gap is now so wide that extraordinary collaboration will be required by both the United States and its key allies in order to arrest the trend and begin to make progress toward more interoperable forces. However the U.S. protects much of its most advanced technologies from being exported. The International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List. These regulations implement the provisions of the Arms Export Control Act. ITAR dictates that information and material pertaining to defense and military related technologies may not be shared with non-U.S. entities without approval from the Department of State. U.S. companies can be fined if they share ITAR-protected products or information such as designs, test data, processes, or software code with foreign partners.

One innovation S&T collaboration with the potential to further interoperability, albeit with a single ally, is the International Technology Alliance (ITA), a research program initiated by the UK Ministry of Defence and the U.S. Army Research Laboratory (ARL).[31] Bilateral collaboration consists of researchers from ARL and the UK MoD working together with several UK- and U.S.-based industries and universities to solve fundamental research problems. ITA research concentrates on four technical areas: a) wireless and sensor networks (ii) interoperability security issues (iii) issues of sensor network information management and (iv) distributed decision making and coalition planning. ITA research is fundamental in nature and focuses on publishing research papers in the public domain. By sticking to fundamental research ITA avoids the issue of ITAR restriction that would hamper research focused on or sponsored by the armed forces of another country.

In additional to the UK, the broader pool of allied support for U.S. military operations is comprised of members of NATO, Australia, New Zealand, and South Korea. An even greater likelihood is that our most frequent interoperable partners will be one of the six fellow members of the Multinational Interoperability Council (MIC)[32] or the even more select four fellow members of the ABCA.[33]

However, many NATO allies have forces that are not postured to be interoperable with the U.S. Army in the near term simply due to domestic limitations on the level of investment in technology. Therefore as an immediate group to engage with, the MIC and ABCA members are the most likely allies to provide interoperable forces alongside the U.S. Army. Heightening interoperability with these allies is a logical place to start.

[31] The 2006 launched ITA is expected to run 10 years. Its full name is United States/United Kingdom International Technology Alliance in Network and Information Sciences. 24 universities and industrial partners from across the United States and UK are involved. The effort is led by IBM Research.

[32] MIC members are Australia, Canada, France, Germany, Italy, the United Kingdom and the United States. New Zealand and NATO's Allied Command Transformation (ACT) have observer status. For more information on MIC see http://www.jcs.mil/j3/mic/

[33] The membership of the 1964 vintage American, Britain, Canadian and Australian Standardization Program (ABCA) has included New Zealand since 1965.

Chapter 7. Conclusions

It is possible to model return on investment for Army Science and Technology (S&T) spending related solely or primarily to adding interoperable capabilities. However, the quantification of ROI must necessarily be framed from underlying qualitative judgments about the value of interoperability that will be in part subjective. There is nothing wrong with such an approach when the metrics are transparent, consistent, and technically acceptable to the user community concerned.

For ROI analysis it is useful to subdivide interoperability investments into those that achieve results intra-Army, in the Joint Force arena, with multinational military partners and finally, with civilian agencies. The latter two categories are likely too general without further defining which allies and civilian agencies are our most likely and frequent partners. Therefore, concentrating interoperability investment on compatibility with the Army's six international MIC partners, and primary civilian partners of the U.S. interagency, makes for a reasoned approach in these areas.

Quantification should focus on numbers of new systems that incorporate all joint and multinational military interoperability standards; on the amount in dollars of S&T investment in system features that provide compliance with Joint and MIC interoperability standards; and on the number of systems designed with integral capacity for additional features that will ensure upgradeable interoperability when an end item is put in the hands of soldiers.

Other criteria can influence the priority of investment in capabilities for joint, multinational, and interagency operations. At present, the Army is engaged in a high level of counterinsurgency OPTEMPO in Iraq and Afghanistan. Based on this type of highly integrated small unit operations, the interoperability of some systems will be more urgent. For example, to enhance interoperability with the U.S. Marines, the Army should protect planned investment in compatible Blue Force Tracking systems through the deployment of the JBC-P system that will finally provide the same information displays on Army and Marine systems. Another priority could be to provide common Army-Marine UAV feeds.

One investment concept that will always be valuable to joint and multinational military interoperability is that of cooperative research and common systems production. Examples of these initiatives include the RQ-7B Shadow UAV acquisition by the Army and Marine Corps and the all-Service Joint Tactical Radio Systems (JTRS). In the international arena cooperative production revolves around issues of technology transfer or of one nation agreeing to procure systems produced by another. While practice is limited by national sensitivities to technology transfer and industrial base protection, there are opportunities that can and have been exploited both by U.S. allies and the United States itself.

The point of decreasing marginal returns on interoperability should be subjected to more in depth research to aid decision makers in determining where to invest limited interoperability resources. It is worthwhile to know where the approximate fault line lies in investing more but realizing less in terms of a system's useful interoperability.

Finally, as much of the discussion in this paper shows, the main return on interoperability for S&T lies in creating greater interoperability with military forces of the other Services

and allies with which the Army most often operates. Far less has been developed with regard to the interoperability with civilian agencies, either within the U.S. government or in the international arena. More research is needed in this area. In particular, what kinds of systems will enhance the Army's collaboration in the field with these agencies? What kinds of communications are required and practical? A critical research requirement will be to gain knowledge of the systems in use by civil agencies.